

FortiExtender Release Notes

VERSION v3.1.2

FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

<http://cookbook.fortinet.com/how-to-work-with-fortinet-support/>

FORTIGATE COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<http://www.fortinet.com/training>

FORTIGUARD CENTER

<http://www.fortiguard.com>

FORTICAST

<http://forticast.fortinet.com>

END USER LICENSE AGREEMENT

<http://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdocs@fortinet.com



5/5/2017

FortiExtender v3.1.2 Release Notes

36-311-308943-20170505

TABLE OF CONTENTS

Change Log	4
Introduction	5
Supported Models	5
What's in FortiExtender v3.1.2	5
Configuration Help	6
FortiGate CLI Configuration	6
FortiExtender-20D CLI Configuration	6
FortiExtender-20D GUI	7
FortiExtender-40D CLI Configuration	7
Upgrade Information	11
Upgrading to FortiExtender v3.1.2	11
Firmware upgrade procedure	11
Firmware mapping to an operator	11
Product Integration and Support	12
Modes of operation	12
Connected UTM mode	12
FortiExtender v3.1.2 support	12
USB modem support	12
FortiExtender-20D	12
Resolved Issues	17
Known Issues	18

Change Log

Date	Change Description
2017-05-05	Minor patch release of v3.1.2 Build 0209.
2017-04-05	Release of v3.1.1 Build 0206.
2017-04-03	Updated from v3.1.0 to v3.1.1 for the second release.
2017-02-02	Initial Release of v3.1.0 Build 0197.

Introduction

This document provides the following information for FortiExtender build 0209:

- [Supported Models](#)
- [What's in FortiExtender v3.1.2](#)
- [Configuration Help](#)
- [Upgrade Information](#)
- [Product Integration and Support](#)
- [Resolved Issues](#)
- [Known Issues](#)

For more information on upgrading your FortiExtender device, see the *FortiExtender Administration Guide*.

Supported Models

FortiExtender supports the following models on GA build 69 or above: FEXT-20D, FEXT-40D-INTL, and FEXT-40D-NAM.



The built-in modems residing in FEXT-40D-NAM and FEXT-40D-INTL can also be upgraded with compatible operator specific modem firmware.

What's in FortiExtender v3.1.2

The following list of features and enhancements were added in v3.1.1 and continue to be supported in v3.1.2:

- By default the FortiExtender-40D-NAM and FortiExtender-40D-INTL can syslog Internet data usage to the FortiGate every Monday or on a monthly basis in MB.
- Access to FortiExtender's web interface via the modem's acquired WAN IP address from the Internet is disabled.
- Upon configuring an Internet data plan, the FortiExtender-40D-NAM and FortiExtender-40D-INTL can syslog data usage levels when it crosses 50%, 75%, 90%, and 100% of the data usage limit.
- On both FortiExtender-40D-NAM and FortiExtender-40D-INTL Internet data overage can be enabled or disabled for a given data plan which can result in continuance or stoppage of the Internet connectivity respectively upon reaching 100% data usage limit.
- Switching between primary and secondary SIMs is now possible based on signal quality, disconnections and Internet data plan usage on both FortiExtender-40D-NAM and FortiExtender-40D-INTL.
- Factory reset of FortiExtender-40D-NAM and FortiExtender-40D-INTL models perform factory resets of the Sierra modem as well.
- Data-usage is displayed on the CLI via the command "get modem data-usage" on both FortiExtender-40D-NAM and FortiExtender-40D-INTL.

Configuration Help

FortiGate CLI Configuration

If an APN were to be configured from the FortiGate this release mandates the configuration of the APN in the format "CarrierName:APN". The below example illustrates the Carrier set to Verizon and APN set to *vzwinternet*.

```
config extender-controller extender
  edit FX04DN4N16000233
    set access-point-name "Verizon:vzwinternet"
    set ppp-username user
    set ppp-password 123
    set ppp-auth-protocol auto
  end
```

FortiExtender-20D CLI Configuration

1. Configuring APN from the FortiExtender-20D CLI which can also help initiate the Cellular Internet data connection despite the absence of the FortiGate APN config or for that matter the absence of the FortiGate itself while operating in bridge mode. The example below illustrates the Carrier set to Verizon and APN set to *vzwinternet*.

```
config modem sim-config
  add Verizon
    set Carrier Verizon
    set APN vzwinternet
    set USER user1
    set PWD 123
    set MODE auto
    set AUTH PAP
  end
```

2. Bridge mode configuration:

- Bridge Mode Enable

```
config system bridge-mode enable
  reboot
```

- Bridge Mode IP

```
config system bridge-mode-ip 192.168.100.2
  reboot
```

Note: The default IP address is 192.168.1.2, unless it is set by the user.

FortiExtender-20D GUI:

- The FortiExtender 20-D GUI home page is displayed below:

FortiExtender FXT20D Dashboard | Configuration | Help

Revision: NTG9X15C_01.13.12.14 r18981 ntgrbc-fwbuild1 2014/07/11 13:48:17
 IMEI: 013323000113762
 IMSI: 310410596203412
 Carrier: AT&T
 Signal Type: DISCONNECTED
 Cell Signal RSSI: -56 dbm
 Cell Signal SINR: NaN dB

General	
Host Name	FXT02D4N16000007 [Change]
Serial Number	FXT02D4N16000007
Firmware Version	FortiExtender-20D v3.1.build0209,170504 (GA)
System Time	Fri May 5 17:33:02 UTC 2017
Uptime	0 min(s)

Device Info	
IP Address	192.168.1.111
Network Mask	255.255.255.0
Gateway IP Address	192.168.1.99
IP Address	192.168.1.99
Device Name	FWF30E3U15000019
State	connected

Hardware (CPU 0.0%, Memory 16.0%)

Home Page accessible at https port 60443 from both WAN and LAN sides with an exception being http accessible only via LAN side.

- The FortiExtender 20-D GUI configuration page is displayed below:

FortiExtender FXT20D Dashboard | Configuration | Help

Network Configuration

Address Mode: ☒ Static ☐ DHCP ☐ Bridge

Default Local IP Address: 192.168.1.2

Default Local Network Mask: 255.255.255.0

Default Gateway IP: 192.168.1.1

SIM Configuration

Carrier/SIM Config: [CARRIER CONFIG] [SIM CONFIG]

CAPWAP Configuration

Discovery Type: ☒ Auto ☐ Static ☐ Broadcast

Extender Controller Port: 5246

Extender Data Port: 25246

FortiGate IP: 192.168.1.1

Firmware Configuration

Extender Upgrade: [Choose File] No file chosen

FortiExtender-40D CLI Configuration

Most carriers in North America can work without any predefined configuration whatsoever, but may need APN config at times when authentication comes into play. Configuring APN, authentication, modem firmware to be used for any given operator on the FortiExtender-40D directly can also help initiate the Cellular Internet data connection without the need of any externally supplied configuration parameters. Currently, barring the APN and

its related authentication parameters, most other parameters like the modem firmware to be used cannot be configured from the FortiGate.

1. Configuring APN and auth parameters with Verizon as an example, and APN as *vzwinternet*. Authentication parameters are to be set on a need basis only. Getting the Carrier Name right is instrumental in making the configuration work well.

```
config modem sim-config
  add Verizon
    set Carrier Verizon
    set APN vzwinternet
    set USER user1
    set PWD 123
    set MODE auto
    set AUTH PAP
end
```

2. Bridge mode configuration:

- Bridge Mode Enable

```
config system bridge-mode enable
  reboot
```

- Bridge Mode IP

```
config system bridge-mode-ip <x.x.x.x>
  reboot
```

3. Signal notification config

- Periodic

```
config modem setting
  set rssi-interval 30 <Periodically reports detailed signal statistics to FortiGate.>
end
```

- Threshold Based

```
config modem setting
  set rssi-threshold 20 <Reports RSSI fluctuations over 20dBm (default is 10dBm).>
```

4. Monitor data-usage statistics

```
get modem data-usage
```

5. Configuring a data plan

```
config modem sim-config
  add 1
    set Slot sim1
    set Data-plan 1000; 13; enable <Data in MB (100- 102400), Billing Date (1-31), overage
    (enable/disable)>
  end
```

6) Enabling the sim-switch while using two sim cards

```
config modem setting
  set sim-switch enable <Enables selection of a sim based on configuration (see Step 7)>
end
```


7)Setting the SIM switch criteria

- Based on disconnections when the sim-switch is enabled (see Step 6).

```
config modem setting
  set switch-on-disconnect 4;600 <No. of disconnects (1-100); evaluation period in seconds (600-18000)>
end
```

- Based on Signal Quality when sim-switch is enabled (see Step 6)

```
config modem sim-config
  add 1
    set Slot sim1
    set Signal -95;600 <Min RSSI value in dBm (-100 to -50); evaluation period in seconds (600-18000)>
  end
```

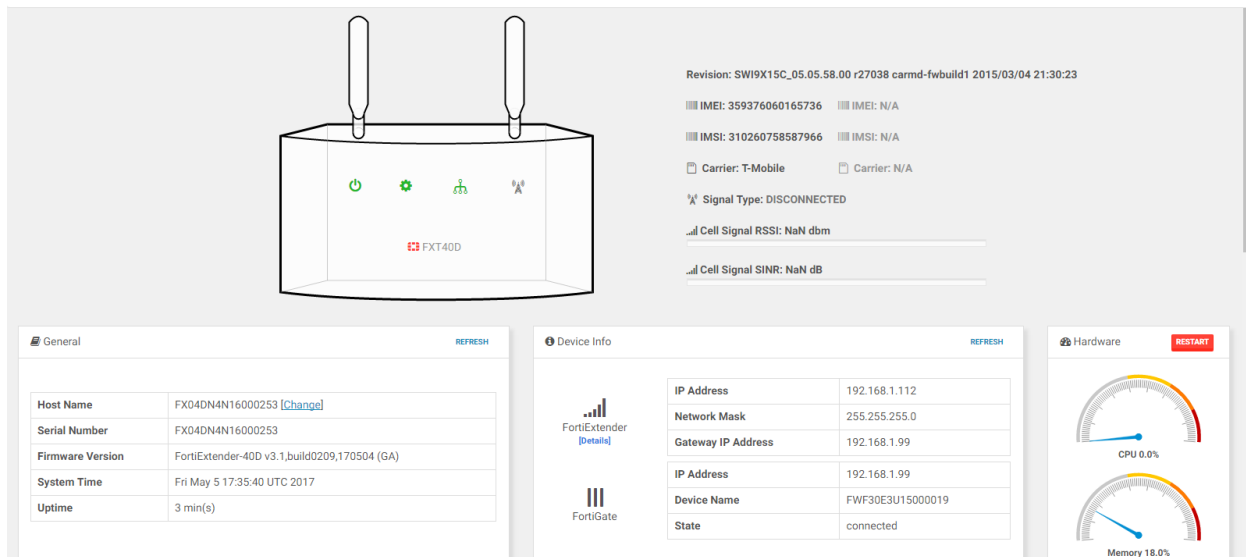
- Based on Data Usage

Please refer to Step 5. Available regardless of the sim-switch parameter being enabled or not.

- The new FortiExtender-40D GUI home page is displayed below:

FortiExtender FXT40D

Dashboard Configuration ? Help



Revision: SWI9X15C_05.05.58.00 r27038 carmd-fwbuild1 2015/03/04 21:30:23

IMEI: 359376060165736 IMEI: N/A

IMSI: 310260758587966 IMSI: N/A

Carrier: T-Mobile Carrier: N/A

Signal Type: DISCONNECTED

Cell Signal RSSI: NaN dbm

Cell Signal SINR: NaN dB

General REFRESH

Host Name	FX04DN4N16000253 [Change]
Serial Number	FX04DN4N16000253
Firmware Version	FortiExtender-40D v3.1.build0209,170504 (GA)
System Time	Fri May 5 17:35:40 UTC 2017
Uptime	3 min(s)

Device Info REFRESH

FortiExtender [Details]

FortiGate

IP Address	192.168.1.112
Network Mask	255.255.255.0
Gateway IP Address	192.168.1.99

IP Address	192.168.1.99
Device Name	FWF30E3U15000019
State	connected

Hardware RESTART

CPU 0.0%

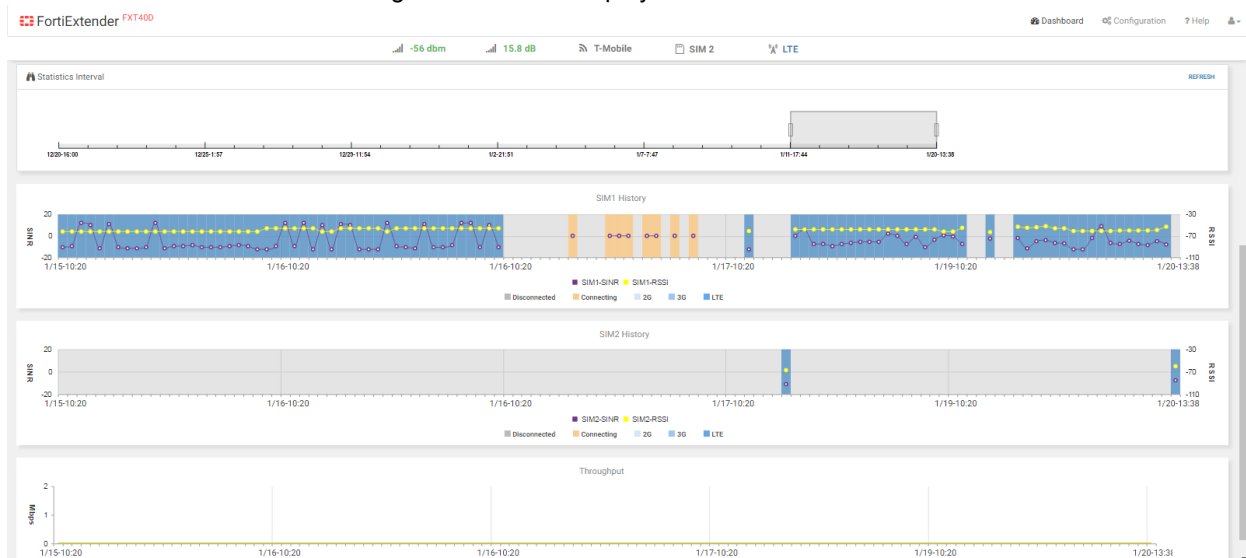
Memory 18.0%

- The new FortiExtender-40D configuration page is displayed below:

The screenshot displays the FortiExtender-40D configuration interface. It features a top navigation bar with 'Dashboard', 'Configuration', and 'Help' links. The main content area is divided into four sections:

- Network Configuration:** Includes fields for Address Mode (Static, DHCP, Bridge), Default Local IP Address (192.168.1.2), Default Local Network Mask (255.255.255.0), and Default Gateway IP (192.168.1.1).
- SIM Configuration:** Includes fields for Default SIM (SIM 1, SIM 2), Carrier Profiles (with a link to 'CLICK FOR DETAILS'), Mapping Mode (Static, Auto), and Carrier/SIM Config (with links to 'CARRIER CONFIG' and 'SIM CONFIG').
- CAPWAP Configuration:** Includes fields for Discovery Type (Auto, Static, Broadcast), Extender Controller Port (5246), Extender Data Port (25246), and FortiGate IP (192.168.1.1).
- Firmware Configuration:** Includes fields for Extender Upgrade (Choose File | No file chosen), SIM Firmware Config (with a link to 'ALL SIM FIRMWARE LIST'), and SIM PRI Config (with a link to 'ALL SIM PRI LIST').

- The new FortiExtender-40D GUI signal statistics is displayed below:



Upgrade Information

Upgrading to FortiExtender v3.1.2

FortiExtender-20D and FortiExtender-40D are capable of operating on v3.0.0 GA build 69 and above.

The built-in modems residing in FEXT-40D-NAM and FEXT-40D-INTL can also be upgraded with compatible operator specific modem firmware.

Firmware upgrade procedure

Firmware Information:

The Sierra EM7355/EM7305 Modem Software comprises of two files:

- A PRL file with the file name ending ".nvu"
- A firmware file with the ending ".cwe"

Both files are required to be flashed onto the Modem to connect to the operator of your choice.

Upgrade instructions and the MODEM firmware have been uploaded to [Fortinet Customer Support site](#) in the download directory under: ".../FortiGate/v5.00/5.4/Sierra-Wireless-3G4G-MODEM-Upgrade/".

Firmware upgrade via the FortiExtender GUI:

1. Login to the web GUI of the FortiExtender with the default credentials. For the username enter *admin* and leave the password blank.
2. In the FortiExtender GUI from in the bottom right corner, click **Sim Firmware Config**.
3. Select the corresponding firmware ending in ".cwe" and flash it.
4. Then, select the corresponding PRI, i.e. the ".nvu" file from **Sim PRI Config** and flash it.
5. After the upgrade is completed, click on the **RESTART** button and confirm with a **YES**.
6. This procedure can take 3 to 5 minutes to finish. Wait for the reboot and make sure the SIM slot is holding the desired SIM.

Firmware mapping to an operator

Once a firmware is uploaded it has to be linked to a Wireless carrier/ operator. Typically a SIM has an IMSI number. The first 6 digits constitute the MCC and MNC will help FortiExtender determine the Carrier of choice most of the time. Otherwise a new entry needs to be created.

Refer to the CLI Help Section for configuration details.

Product Integration and Support

Modes of operation

FortiExtender supports Connected UTM and Standalone modes of operation.

Connected UTM mode

This is the default mode of operation where the FortiGate provides centralized management of the FortiExtender infrastructure. In this mode the device discovers the FortiGate using the CAPWAP protocol and WAN traffic is tunneled to the FortiGate's wireless WAN virtual interface. For connect UTM mode, FortiGates must run FortiOS v5.2.0 or later.

FortiExtender v3.1.2 support

The following table lists FortiExtender product integration and support information.

FortiExtender 3.0.2 Support	
Web Browsers	Microsoft Internet Explorer versions 10 and 11
	Mozilla Firefox version 33
	Other web browsers may function correctly, but are not supported by Fortinet.
FortiOS/FortiOS Carrier	v5.2.0 and later
FortiManager	v5.0.7 and later
	v5.2.0 and later

USB modem support

The following tables list USB modems that are supported for various models.

FortiExtender-20D

The following table lists USB modems that are supported by the FortiExtender-20D:

Brand	Modem Model	Operator / Area
Netgear	340U	AT&T (USA)
Sprint	341U	Sprint (USA)
Sierra	313	AT&T (USA)
Pantech	295	Verizon
ZTE	820B	Claro (Puerto Rico)
ZTE	MF683	T-Mobile
Novatel	MF620L	Verizon
Huawei	E398	Any GSM/LTE
Huawei	UMG1691	T-Mobile
Huawei	E173	Any GSM, 3G, HSPA network
Huawei	E3276	Any GSM/LTE
TPLINK	MA260	Any GSM/3G
TPLINK	MA180	Any GSM/3G
ZTE	K3520-Z	HSDPA, WCDMA
ZTE	K3563-Z	
ZTE	K3565-Z	HSDPA 3.6/0.38
ZTE	K3570-Z	HSDPA 3.6/0.38
ZTE	K3571-Z	HSDPA 7.2/0.38
ZTE	K4505-Z	HSPA+ 21.6/5.76
ZTE	K5006-Z	LTE CAT3
ZTE	MF30	HSDPA 7.2 HSUPA 5.76
ZTE	MF60	HSPA+ 21.6/5.76
ZTE	MF100	HSDPA 3.6/0.38
ZTE	MF110	HSDPA 7.2 HSUPA 5.76

Brand	Modem Model	Operator / Area
ZTE	MF112	HSDPA 7.2 HSUPA 2.0
ZTE	MF170	HSDPA 3.6/0.38
ZTE	MF190	HSDPA 7.2 HSUPA 2.0
ZTE	MF626	HSDPA 3.6/0.38
ZTE	MF627	HSDPA 7.2 HSUPA 5.76
ZTE	MF632	HSDPA 7.2 HSUPA 3.6
ZTE	MF633	HSDPA 7.2 HSUPA 5.76
ZTE	MF636	HSDPA 7.2 HSUPA 5.76
ZTE	MF637	HSDPA 7.2 HSUPA 5.76
ZTE	MF637U	HSDPA 7.2 HSUPA 5.76
ZTE	MF662	HSPA+ 21.6/5.76
ZTE	MF668	HSPA+ 21.6/5.76
ZTE	MF668A	HSPA+ 21.6/5.76
ZTE	MF669	HSPA+ 21.6/5.76
ZTE	MF680	DC-HSPA+ 42.2/5.76
ZTE	MF683	DC-HSPA+ 42.2/5.76
ZTE	MF820D	LTE CAT3
ZTE	MF821	LTE CAT3
ZTE	MF821D	LTE CAT3
ZTE	MF880	LTE CAT3
ZTE	MT505UP	HSUPA
ZTE	MT512HS	HSDPA 7.2 HSUPA 3.6
ZTE	MT8205	LTE CAT3
HUAWEI	B81	HSDPA 7.2 HSUPA 5.76

Brand	Modem Model	Operator / Area
HUAWEI	D33HW	HSPA+ 21.6/5.76
HUAWEI	D41HW	DC-HSPA+ 42.2/11.5
HUAWEI	E153	HSDPA 3.6/0.38
HUAWEI	E156G	HSDPA 3.6/0.38
HUAWEI	E171	HSDPA 7.2 HSUPA 5.76
HUAWEI	E173	HSDPA 7.2 HSUPA 5.76
HUAWEI	E180V	HSDPA 7.2 HSUPA 5.76
HUAWEI	E200	HSDPA 3.6
HUAWEI	E261	HSDPA 7.2 HSUPA 5.76
HUAWEI	E270+	HSPA+ 21.6/5.76
HUAWEI	E303F	HSPA+ 21.6/5.76
HUAWEI	E352	HSPA+ 21.6/5.76
HUAWEI	E353W-u1	HSPA+ 21.6/5.76
HUAWEI	E367	DC-HSPA+ 28.8/5.76
HUAWEI	E372	DC-HSPA+ 42.2/5.76
HUAWEI	E389	LTE CAT3
HUAWEI	E392	LTE CAT3
HUAWEI	E398	LTE CAT3
HUAWEI	E398u-15	LTE CAT3
HUAWEI	E1552	HSDPA 3.6/0.38
HUAWEI	E1690	HSDPA 7.2 HSUPA 5.76
HUAWEI	E1691	HSDPA 7.2 HSUPA 5.76
HUAWEI	E1692	HSDPA 7.2 HSUPA 5.76
HUAWEI	E1731Bu-1	HSPA+ 21.6/5.76

Brand	Modem Model	Operator / Area
HUAWEI	E1762	HSDPA 7.2 HSUPA 5.76
HUAWEI	E1800	HSDPA 7.2 HSUPA 5.76
HUAWEI	E1815	HSPA+ 21.6/5.76
HUAWEI	E1820	HSPA+ 21.6/5.76
HUAWEI	E1823	HSPA+ 21.6/5.76
HUAWEI	E3131s-2	HSPA+ 21.6/5.76
HUAWEI	EC122	CDMA2000
HUAWEI	EC176-2	CDMA EV-DO Rev.A
HUAWEI	EC178	CDMA EV-DO Rev.A
HUAWEI	EC189	HSDPA 7.2 HSUPA 5.76
HUAWEI	EC306	HSPA+ 21.6/5.76
HUAWEI	EC1270	DC-HSPA+ 42.2/11.5
HUAWEI	Speedstick LTE	HSDPA 3.6/0.38

Resolved Issues

The following issues have been fixed in version v3.1.2. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Bug ID	Description
0415454	Custom APN fix for carriers requiring Generic firmware like Saskatel.
0421745	Use of Generic modem firmware for small wireless carriers like Saskatel.
0417308	Reverting to CAPWAP mode from configured VLAN mode while swapping SIM cards

Known Issues

The following issues have been identified in v3.1.2. For inquiries about a particular bug, please contact [Customer Service & Support](#).

FortiExtender 40D:

Bug ID	Description
N/A	[Sprint Cert] missing fields like DRC, PN code, PN offset, etc. in EVDO AT command output.
N/A	Physical insertion of a SIM requires a FortiExtender-40D power cycle.

FortiExtender 20D:

Bug ID	Description
N/A	Physical insertion of a modem requires a FortiExtender-20D power cycle.
N/A	FortiExtender mode change from CAPWAP to VLAN or vice-versa requires a power cycle.



High Performance Network Security



Copyright© 2017 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.